Yphise portfolio of valuable projects
Independent research since 1985

Software Product Assessment EXECUTIVE VOLUME

SELECTED BUSINESS CASE

COMPLIANCE MANAGEMENT

UBCA - USER BEHAVIOR COMPLIANCE AUDIT

For guaranteeing the compliance and integrity of sensitive operations

GM Governance	**IS** Information Systems
PR Projects	**SO** Service Management

Yphise is committed to providing IT executives and managers with the best independent research on methods and solutions to optimize IT performance.

Yphise is an independent company that conducts ongoing research programs for IT executives and managers. Yphise has a dedicated research team in order to guarantee independence, consistent results and timely updates.

Yphise clients include over 900 major companies worldwide. They come from all sectors, including manufacturing, banking, insurance, retail sales, transportation, services and government.

Yphise conducts two exclusive ongoing research programs

1. Comparative assessment of software solutions

Yphise identifies and certifies the software solutions that allow large companies to increase the value of their information systems while optimizing the costs and managing the risks. Yphise covers all areas of interest to develop, operate, maintain and secure the applications to compete. Yphise has assessed 150 software solutions each year since 1985. This program is ISO 9001:2000-certified in order to guarantee independence and accurate focus on key issues for large companies.

2. Assessment of operational practices and methods

Yphise provides IT executives and managers with an open framework of operational best practices aimed at optimizing the IT cost, value and risk. It covers all IT missions in order to guarantee effective operational management. It uses a pragmatic approach. It includes a scoring model for easy periodical self-assessment. This leads to immediate improvement of each IT process through use of the released best practices.

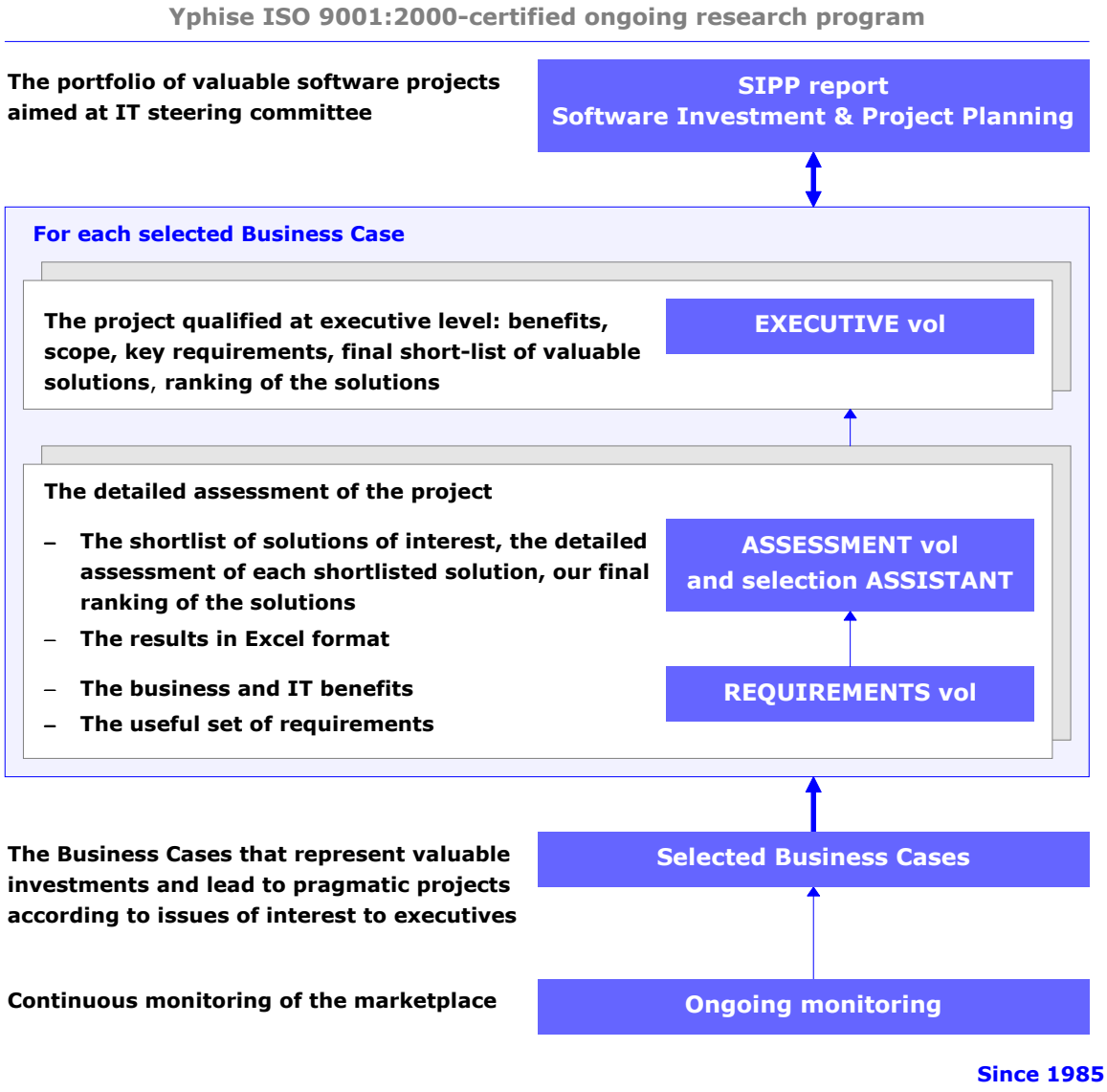
yphise@yphise.com

PO BOX 142, Southbury, CT 06488 - USA T 1 203-405-2549 - F 1 203-405-2569

6 rue Beaubourg - F-75004 PARIS T (33) 1 44 59 93 00 - F (33) 1 44 59 93 09

FOREWORD

The EXECUTIVE volume summarizes the results of independent research conducted by Yphise on the assessed business case.



This business case has been selected under the Yphise ongoing research program, which identifies the software solutions that represent a valuable investment for large companies. The EXECUTIVE volume defines the project at the executive level. It establishes the benefits, scope, key requirements, as well as a final short list of solutions with proven strengths.

The Yphise ongoing research program has helped executives plan, prioritize, conduct and control the useful software projects in order to increase IT performance since 1985.

– This program covers all areas of interest to large companies. Yphise has unparalleled experience in identifying those business cases that represent valuable investments and projects.

GM IT Governance and Management

- Method and quality management
- IT financial and asset management
- IT risk control
- Outsourcing strategies
- Business Partnership management
- Demands and project portfolio mngt

IS Information System Management

- Architecture
- Industrializing
- Security

PR Conducting Projects

- Conducting projects
- Architecture
- Industrializing
- Security
- Testing
- Maintenance
- Service Continuity
- Service level management

SO Service and Operations Management

- Change and release management
- Environment delivery
- Operations
- Help-desk, incidents, problems
- Service Continuity
- Service level management

– This program is ISO 9001:2000-certified (since 1999). This unique distinction demonstrates independence and a robust methodology for assessing software solutions according to the priorities of large companies.

The Executive License grants IT executives, software vendors and service providers with online access (www.yphise.com) to all the EXECUTIVE vols and to the SIPP (Software Investment & Project Planning) report.

BENEFITS

User Behavior Compliance Audit (UBCA) solutions manage and automate the audit of operations performed by users through IT services, in order to check compliance with corporate policies and with legal and regulatory requirements. They mitigate the risk of internal fraud. They check the dynamic compliance of the IT, i.e. whether the way it is used is on the level.

UBCA solutions collect logs, audit trails and data from heterogeneous sources. They centralize them while guaranteeing their integrity. They store this huge volume of data. UBCA solutions translate high-level business-centric compliance criteria into a complex combination of IT criteria. They correlate events and define the patterns and, thus, the policies corresponding to aboveboard behaviors. They support investigation and audit in order to detect whether user behaviors are aligned with the regulatory requirements and company policies.

UBCA solutions contribute to ITIL strategies. ITIL v3 is the worldwide reference for service management, which is a key factor in aligning the IT on business needs. ITIL v3 Service Design processes include information security management (§ 4.6 in Service Design). The description of this process states that information security management systems must supervise and check compliance with the security policy and security requirements in SLAs and OLAs, as well as provide information to external auditors and regulators. This is the purpose of assessed solutions.

UBCA may also be called security information management (SIM). However, this wording is highly ambiguous. The key interest of these solutions lies not in operational IT security but in effective governance, risk mitigation and compliance audit. This is why we prefer to refer to user behavior compliance audit, which is much more accurate, precise and well-centered than SIM is.

Benefits for the business

Our research shows that UBCA solutions are a key investment in order to guarantee effective governance, risk mitigation and compliance with legal and regulatory frameworks. UBCA solutions are essential to mitigate the risk of irregular business operations.

- **Demonstrating the operation compliance with corporate policies**

  Corporate governance requires demonstrating the compliance of operations with all relevant policies, i.e. regulatory and legal framework, corporate strategy policies and security policies. Executives are accountable for this compliance. The capability to demonstrate compliance at any time is a key benefit in terms of legal compliance, of investor trust and of compliance audit costs.

  Demonstrating the operation compliance requires knowing exactly what is happening, i.e. how operations are running. This requires fully qualified, reliable information from

all applications, services and IT infrastructure components. The key point is not how these components are configured but how they are used, i.e. how users behave. This represents huge volumes of data to be collected from log files and audit trails. Demonstrating the operation compliance with corporate policies requires effective and efficient collection of data on how the information system is actually used.

Demonstrating the operation compliance requires identifying, in all the available elementary data, the meaningful behavior with regard to compliance criteria. On the one hand, this requires translating high-level business-centric compliance criteria into a rich and complex combination of IT criteria. On the other hand, this requires efficient detection of patterns previously defined within the volumes of collected data.

Demonstrating the operation compliance requires proving that operations were conducted as claimed. This requires long-term, reliable archiving of proof. This requires non-repudiable proof.

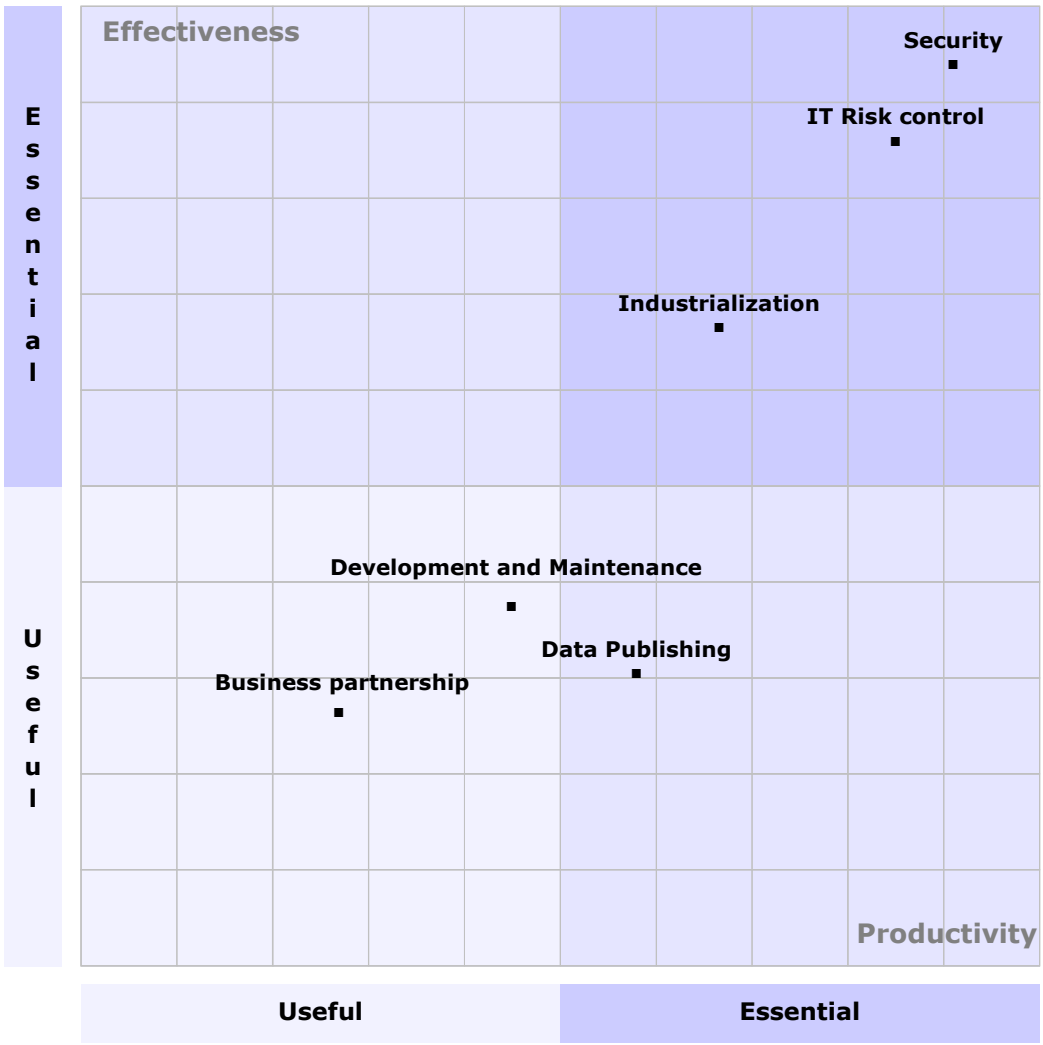
- **Reducing the cost of fraud**

Noncompliant operations are close to frauds. Noncompliant user behavior may be used to steal money or information, may lead to a loss of customers or partners, or may degrade the corporate image.

Reducing the cost of fraud requires detecting the frauds, as explained in the benefit above.

Reducing the cost of fraud also requires investigating the suspect behavior in order to accurately understand what is happening and the root cause. This helps in responding to frauds, thereby reducing the cost and duration of frauds.

Benefits for the IT processes



Benefits for the IT processes

- **Security**

The security process guarantees the confidentiality, authentication, integrity and nonrepudiation of data, content and processes, as well as protection against security threats.

UBCA solutions help ensure that the key challenges of the security process are met. They guarantee that user behaviors are aboveboard. This mitigates the risk of fraud and ensures compliance of operations with regulatory requirements. UBCA solutions make it possible to turn technical security events into meaningful business-oriented compliance or noncompliance events.

- **IT risk control**

  IT governance requires managing the risks that information systems represent for a company. Companies must guarantee compliance with regulatory requirements (e.g. the S*arbanes-Oxley Act*). The IT risk management process identifies and assesses the risks in order to provide executives with an accurate understanding of the current situation. It defines and monitors the strategies for mitigating the IT risk.

  UBCA solutions help comply with regulatory frameworks. They focus on risk consecutive to human behavior with IT services. They design policies in order to model the expected behavior and provide accurate reporting on specific situations. UBCA solutions make it possible to track compliance accurately and reliably over time. They enable the IT to provide the whole company with timely and useful information in case of legal prosecution or investigation.

- **Industrialization**

  The industrialization process must ensure that the information system operates according to the service level expected by the business. In each application project, the industrialization process develops the operational tools and instructions required for deployment and operations. It designs and manages technical solutions aimed at guaranteeing the effectiveness in operations.

  One of the key challenges of industrialization is the monitoring and mitigation of operational risks. UBCA solutions rely on tools and operational instructions provided by the industrialization in order to define policies, i.e. authorized or prohibited actions. UBCA solutions reduce the work involved in implementing specific logs, audit trails, as well as collection and analysis tools for risk detection and monitoring. They significantly reduce the industrialization workload in projects.

- **Data publishing**

  The data publishing process must guarantee data publishing and propagation from business intelligence systems (datamarts, data warehouses) or collaborative systems (intranet, document management systems).

  UBCA solutions help guarantee the integrity of data before publication or propagation. They track, sign and protect the data necessary to demonstrate compliance, from creation to publishing.

- **Business partnership management**

  The business partnership management process must guarantee the collection, understanding and processing of business needs. Collaboration of business units with the IT department often fails due to a lack of common wording and reference.

  UBCA solutions enable the IT to deliver new services to the business. Compliance audit is a key issue for the business. The solution proposed by the IT used to be limited to

technical log management. UBCA solutions bridge the gap between technical events and business compliance.

- **Development and maintenance**

  A key development challenge is productivity, i.e. releasing the applications on time and within budget. A key challenge of maintenance is the guarantee of non-regression of existing information systems when budgets and time frames are tight.

  UBCA solutions avoid all the development dedicated to log-specific information for behavior tracking and to behavior analysis. Without UBCA solutions, user behavior compliance audit requires specific development as well as maintenance. This development makes the application code more complex and, therefore, more difficult to maintain.

YPHISE SHORTLIST

Positioning of the market segment

The evaluated market segment is a specific one, with a precise positioning and list of solutions. To avoid confusion, we differentiate it from the following list of market segments. A solution belonging to one of these market segments is inappropriate for attaining the expected benefits.

- **Security event management (SEM) solutions**

  SEM solutions provide a real-time security monitoring console. They act immediately in case of attack.

  SEM solutions provide real-time information and alert in case of threat. They are designed for security managers and operators. UBCA solutions provide in-depth analysis based on long-term storage. UBCA solutions are designed for risk management and auditors.

  Some solutions in the marketplace cover both UBCA and SEM.

  E.g. Enterprise Security Manager (Arcsight), Security Manager (Attachmate), Symantec Security Information Manager (Symantec), EventMAnager (Exaprotect) and Tivoli Security Operations Manager (IBM).

- **Server configuration compliance audit (SCCA) solutions**

  Server configuration compliance audit (SCCA) solutions check, control and score the compliance of server and desktop configurations against configuration and security rules. These rules can be specific to the company or based on standard frameworks and best practices.

  SCCA solutions focus on static configuration compliance. UBCA solutions focus on dynamic compliance, i.e. compliance of the way IT services are used. SCCA solutions reduce the vulnerability, while UBCA solutions reduce the threat. SCCA solutions and UBCA solutions are complementary tools in order to ensure the compliance audit of the information system.

  E.g. CCS & ESM (Symantec), NetIQ Secure Configuration Manager (Attachmate) and Tivoli Security Compliance Manager (IBM).

- **Access management (AM) solutions**

  AM solutions manage user authentication. They authorize or deny access to services, according to customized rules. They rely on an enterprise directory to authenticate the user identifiers.

AM solutions focus on rule enforcement, i.e. they force operations to be performed in a compliant way. They do not control or audit user behaviors in sensitive operations. UBCA solutions do not control access to desktops and servers. AM solutions and UBCA solutions are independent tools.

E.g. BMC Access Manager (BMC), OpenView Select Access (HP), RSA Access Manager (RSA Security), Sun Access Manager (Sun Microsystems) and Tivoli Access Manager (IBM).

- **Network access protection (NAP) solutions**

NAP solutions protect the private network of a company by enforcing the compliance with computer security requirements. They allow network access or communication. They can confine unsecured computers to a restricted network until they become secure. NAP solutions do not manage the IT infrastructure.

NAP solutions focus on ensuring the network security compliance. They grant access or not to the computer. They provide remediation in case of risk. They provide real-time information. NAP solutions and UBCA solutions are complementary tools.

E.g. Cisco Trust Agent (Cisco), Microsoft NAP (Microsoft) and Symantec Network Access Control (Symantec).

- **Security vulnerability management (SVM) solutions**

SVM solutions discover and manage devices and applications on the network. They identify and remove network security vulnerabilities. They measure and manage security exposure and risk. SVM solutions specialize in securing the network.

SVM solutions focus on checking or scoring server configuration compliance. SVM solutions ensure that the configuration is compliant, while UBCA solutions ensure that use of the information system is compliant. Both solutions are aimed at demonstrating the compliance based on standard frameworks, but they have a different focus. UBCA solutions and SVM solutions are complementary tools.

E.g. IBM Internet Scanner Software (IBM), QualysGuard (Qualys) and Vulnerability Manager (Computer Associates).

- **Network scanner solutions**

Network scanners explore the network in order to identify available hosts, hosted services, running operating systems, and firewalls in use.

Network scanners secure the information system against misconfiguration of security items. Network scanners prevent risks from a technical point of view, while UBCA solutions prevent internal risks from a business point of view. They can be complementary in case of investigation consecutive to a fraud.

E.g. NMap (Open source).

- **Antivirus solutions**

  Antivirus solutions rely on a consistent and updated antivirus database to detect in real time the presence of viruses, worms and Trojan horses. They help remove the vulnerabilities due to such malware.

  UBCA solutions track the internal risk or fraud and provide an after-the-fact analysis of user behaviors. Antivirus solutions are aimed at protecting against the external risk of the information system. UBCA solutions and antivirus solutions are complementary tools to ensure the security of the information system.

  E.g. Norton AntiVirus (Symantec), McAfee Antivirus (McAfee), Endpoint Security and Control (Sophos) and InterScan (TrendMicro).

- **Host-based intrusion detection system (HIDS)**

  HIDSs are intrusion detection systems that monitor and analyze the internal parameters and state of systems (the stored information, RAM).

  UBCA solutions investigate after the fact, while HIDS solutions work on real-time information. HIDS solutions do not analyze the risk arising from user behavior and do not provide reporting. UBCA solutions can rely on an HIDS for the monitoring of computing systems.

  E.g. OSSEC and Samhain.

- **Federated identity management (FIM) solutions**

  The purpose of FIM solutions is to set up partnerships. Partners may be various companies or departments within the same company. FIM solutions manage the relationships between service providers, service consumers and identity providers. They communicate credentials information between partners.

  FIM solutions certify the identity of end-users and their right to access services. UBCA solutions correlate this information with logs and usual behavior to determine whether something seems suspect. UBCA solutions and FIM solutions are complementary.

  E.g. BMC Identity Management Platform (BMC Software), HP Select Federation (HP), Sun Federation Manager (Sun Microsystems) and Tivoli Federated Identity Manager (IBM).

- **Identity provisioning and management (IPM) solutions**

  IPM solutions manage the definition of users, accounts and access rights. They create accounts in the various user repositories, as required by the role of each user. They fill in the information according to data keyed in only once, not keyed in each repository. They synchronize various user repositories; data on users changed centrally or locally is propagated to the other user repositories to ensure data consistency. IPM solutions grant the appropriate access rights automatically according to business roles and

without switching to another access management interface. They automatically revoke the access rights and delete the accounts of leaving users: they ensure that no access deletion is forgotten.

UBCA solutions do not manage the definition of users, accounts and access rights. However, they can retrieve identities from IPM solutions. UBCA solutions rely on the access rights to define the normal or abnormal behavior of users.

E.g. BMC Identity Management Platform (BMC), CA Identity Manager (CA), HP Select Identity (HP) and Tivoli Identity Manager (IBM).

- **SOA runtime security (SRS) solutions**

SRS solutions centralize management of security policies within the information system. They secure access to applications, software components and business data.

SRS solutions protect the data, while UBCA solutions demonstrate that the user behaviors are compliant with regulatory frameworks and company policies.

E.g. BEA AquaLogic Enterprise Security (BEA) and Actional for Active Policy Enforcement (Progress Software).

- **Service monitoring and management (SMM) solutions**

SMM solutions optimize the service runtime in service-oriented architectures (SOAs). They enforce performance and security of running services through policies. Policies define rules and actions in order to control service behavior. Policy management is critical for SOA runtime governance. Policies help control the availability, response time and security of services. SMM solutions make it possible to create and deploy policies to the running services. SMM solutions monitor the running services. They collect metrics on service execution, such as availability, performance, call frequency or number of errors. They measure how the services run in each layer: service containers, applications, services and service operations. They help analyze the root cause upon incidents.

In terms of security, SMM solutions focus on the running of the services. UBCA solutions deal with user behavior within an information system and with fraud detection. They both focus on the risk arising from within information system. SMM solutions mitigate this risk from a technical point of view, while UBCA solutions focus on the risk from a business point of view.

E.g. Amberpoint SOA Management System (Amberpoint), Progress Actional (Progress Software), Service Manager (SOA Software) and ActiveMatrix Policy Manager (Tibco).

- **Business intelligence (BI) solutions**

BI solutions help managers, business operators or analysts analyze business activity for decision making. They focus on providing user-friendly functions for querying and reporting the data stored in data warehouses, datamarts or operational systems.

BI solutions help understand business activities by querying and manipulating operational data. BI solutions focus on what happens, not on who performs what and when. UBCA solutions ensure that the operational data is compliant with regulatory frameworks and corporate policies. They are independent solutions.

E.g. BusinessObjects (BusinessObjects), DBA Alphablox (IBM) and SAS Business Intelligence (SAS institute).

- **Strategic performance management (SPM) solutions**

SPM solutions help assess enterprise performance according to strategic objectives. SPM solutions help define financial and nonfinancial objectives and the best strategies to meet these objectives. Strategies include all actions to be implemented in order to meet the objectives. SPM solutions help executives and managers define, implement and monitor their strategies. They help identify and plan subobjectives, projects and tasks pertaining to the strategy according to resources. They help communicate the strategy to the whole company. They deliver scorecards or dashboards in order to control strategy implementation and progress toward objectives.

SPM solutions help define and manage the best strategy according to objectives. UBCA solutions guarantee that the data is consistent. UBCA solutions help ensure that the strategic objectives are computed according to consistent information. UBCA solutions help guarantee that the strategic objectives are true.

E.g. Cognos 8 Business Intelligence (Cognos), Business Objects EPM (Business Objects), Hyperion System 9 (Hyperion/Oracle) and SAS Strategic Performance Management (SAS).

The short list for the evaluated business case

We selected this business case in the Yphise portfolio of project opportunities for the first time. UBCA solutions are an essential foundation for demonstrating and checking the compliance with the company policies and the demanding regulatory frameworks in terms of security.

The ISO 9001:2000 certification of our process is evidence of independence and robust methodology for assessing the solutions according to issues and priorities of large companies. All shortlisted vendors demonstrate their commitment to responding to the requirements of this process. This process challenges them, as in a customer situation. It is evidence of the vendors' commitment to responding to a demanding independent assessment.

Our final short list is as follows:

- NetIQ Security Manager (Attachmate);
- enVision (EMC/RSA);
- EventManager (Exaprotect);
- Symantec Security Information Manager (Symantec); and
- Tivoli Compliance Insight Manager (IBM).

The shortlisted vendors come mainly from the IT security. The shortlisted solutions are usually included in IT security portfolio. However, we insist on the actual positioning of these solutions: they are not security solutions; they are governance, risk and compliance solutions.

Due to this history of the vendors, some confusion with SEM and SCCA is possible. The UBCA business case is complementary to the SEM and SCCA business cases, but distinct.

- **NetIQ Security Manager, Version V6.0 SP2 (Attachmate)**

  Attachmate is a private company. It focuses on providing proven systems and security management solutions. Attachmate is committed to three segments: enterprise system and application management, operational monitoring and security for Vmware and security and compliance management.

  In 2006, Attachmate acquired NetIQ, including Security Manager, which is now part of the security and compliance management segment. The solution may be complemented with additional modules for specific systems such as Change Guardian for Windows (for auditing changes on files system), Change Guardian for Active Directory (for auditing changes according to role) and Group Policy Guardian (for auditing changes according to Microsoft Group policy).

- **enVision, Version V3.7 (EMC/RSA)**

  EMC focuses on information lifecycle management (ILM). ILM includes security of the involved information. RSA focuses on information risk management.

  RSA has became the EMC security division in September 2006. Its portfolio includes identity insurance (strong authentication), Data Loss Prevention and Security Information and Event Management (enVision offer). Version 3.7 of enVision was released in January 2008.

- **EventManager, Version 3.0 (Exaprotect)**

  Exaprotect is a privately held and venture-backed organization. Exaprotect provides solutions to design, deploy, analyze and provide remediation to security policies in large-scale, heterogeneous environments. It focuses on UBCA and SEM. Version 3 of EventManager was released in June 2008.

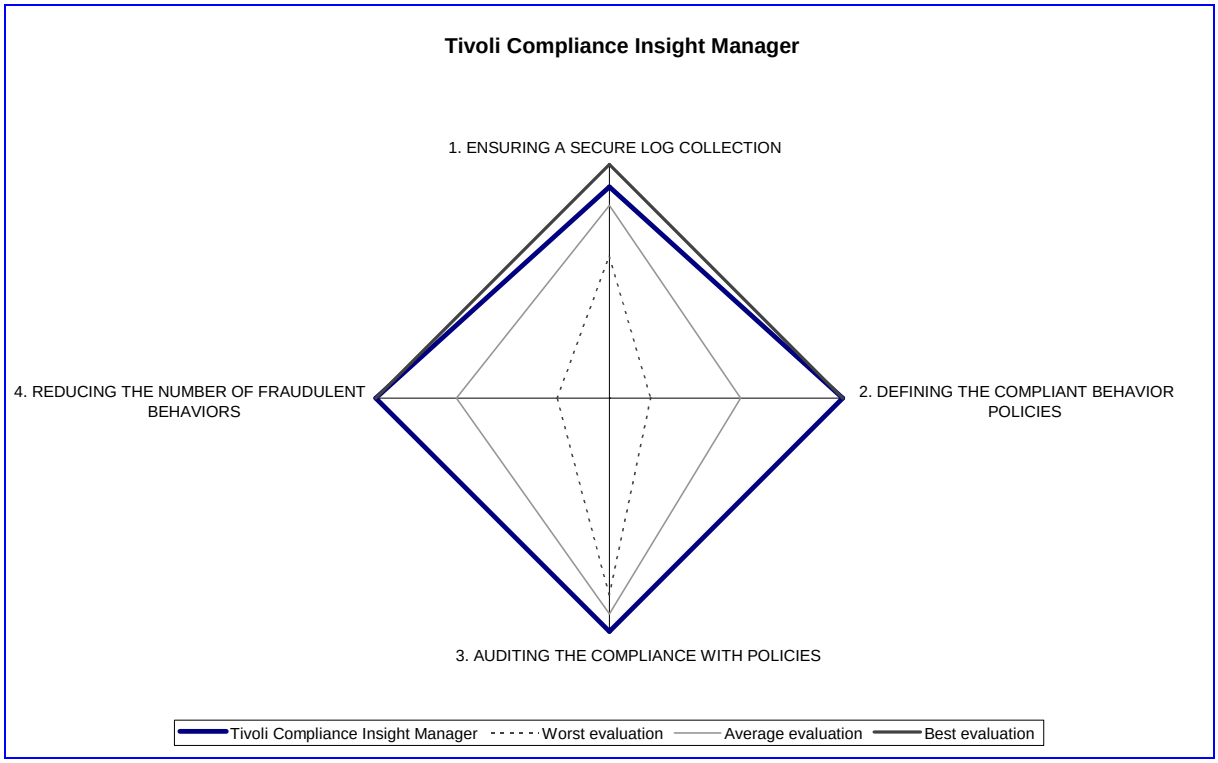
- **Symantec Security Information Manager, Version 4.6 (Symantec)**

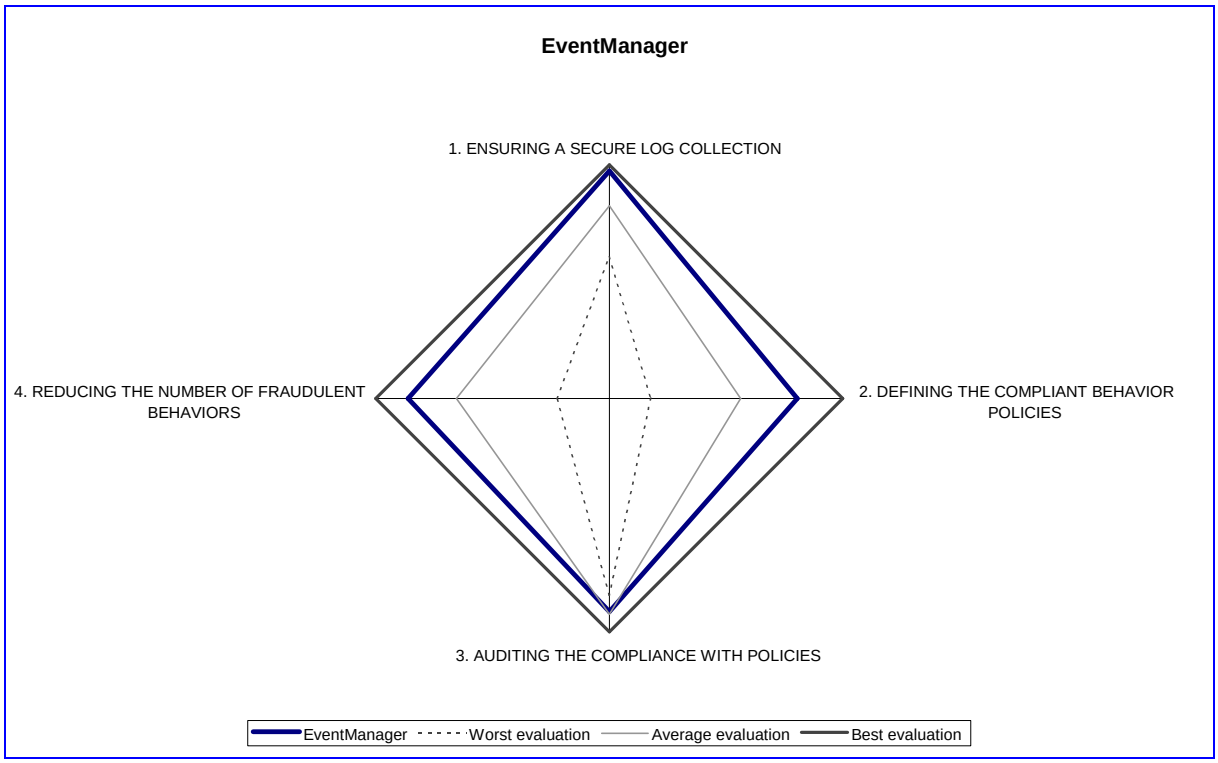
  Symantec delivers solutions to help businesses and consumers protect their infrastructure, information and interactions. The main significant strategic business units of Symantec are the following: consumer products (for delivering Internet security), security and data management, data center management and services. Symantec Security Information Manager is part of security data management.

- **Tivoli Compliance Insight Manager, Version 8.5 (IBM)**

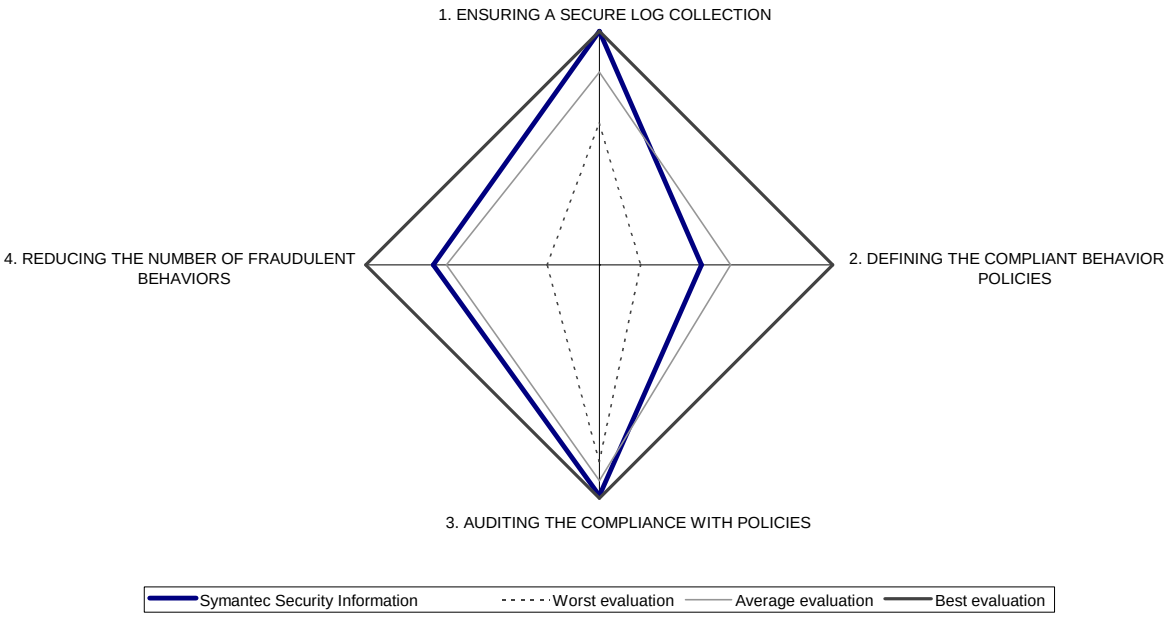
  Tivoli is the IBM software business line dedicated to infrastructure management i.e. storage, security, automation management and provisioning. IBM acquired Micromuse in 2006 and Consul in 2007 to strengthen its security information and event management offering. Tivoli Compliance Insight Manager is the new name of the solution acquired through Consul. The IBM Tivoli Security Information and Event Management (SIEM) portfolio is composed of Tivoli Secure Operation Management and of Tivoli Compliance Insight Manager.

YPHISE RANKING

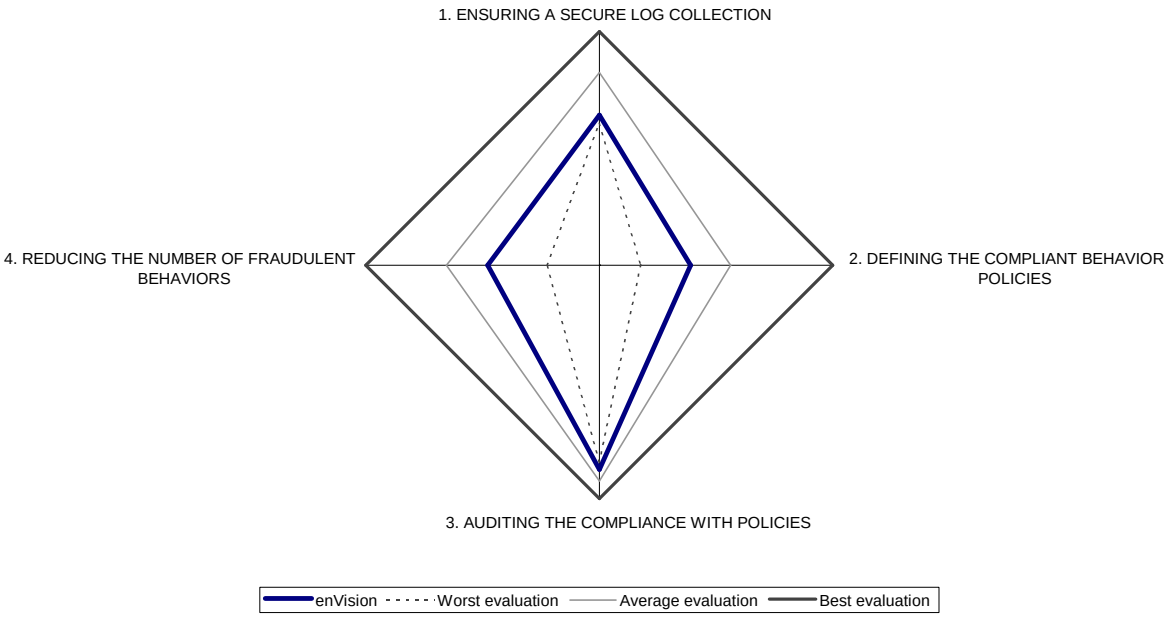


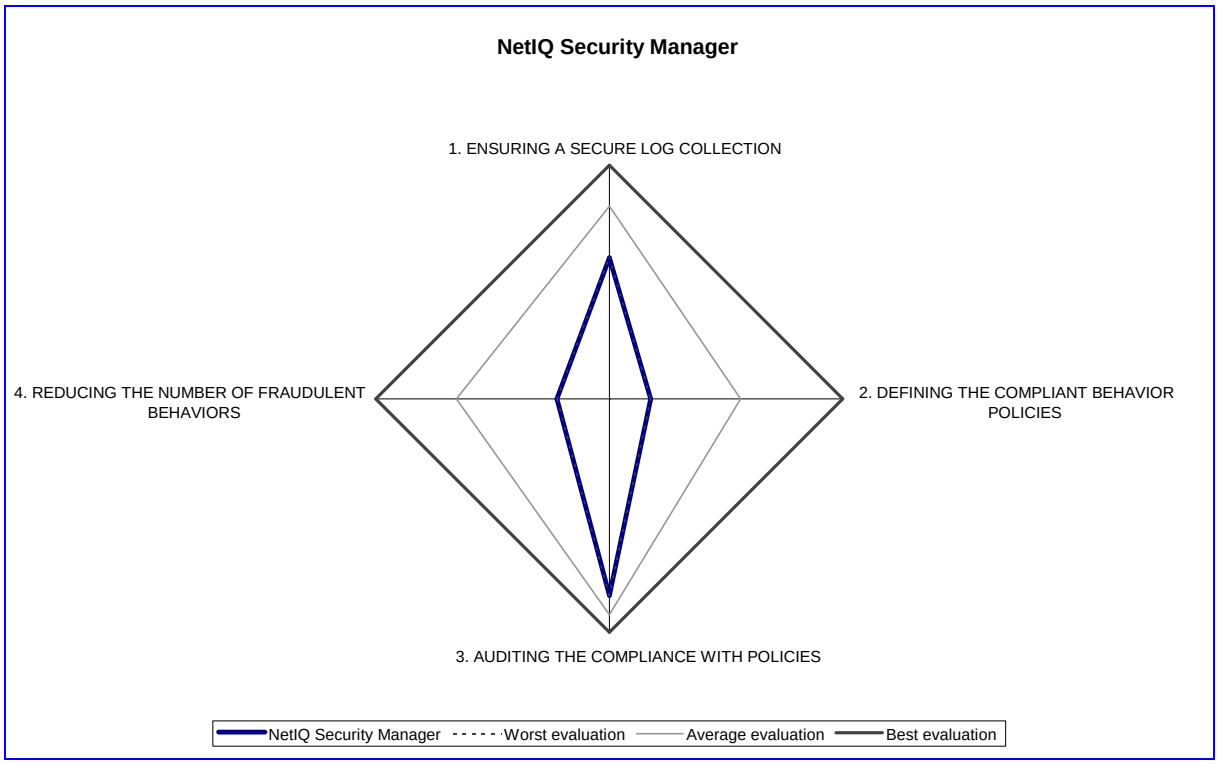


Symantec Security Information Manager



enVision





The above charts are presented in order of final top-down ranking of the shortlisted solutions after their in-depth ISO 9001:2000-certified assessment by Yphise.

The four assessment dimensions show the expected benefits by large companies. They aggregate more than 150 functional or technical control items. This list of requirements is practical, in order to evaluate the capacity of the solutions to provide an adequate return on investment. It is also proactive in order to appreciate the upcoming perspectives.

Assessment dimensions

1. Ensuring a secure log collection

Demonstrating the compliance with corporate policies requires collecting the elementary data on the events, behaviors and actions. UBCA solutions must collect logs from any required data source, regardless of the heterogeneity of sources and the volume of data. They must ensure the integrity of this data. They must store this data securely for long-term use and proof.

2. Defining the compliant behavior policies

Compliance with corporate policies is tied to user compliance with behaviors considered to be on the level. These behaviors are defined by data from various systems, which needs to be aggregated and correlated. UBCA solutions must centralize and normalize the data. They must manage behavior patterns that constitute the policies. They must compare the collected data to the patterns. They must manage the policy lifecycle.

3. Auditing the compliance with policies

Demonstrating the operation compliance requires providing quick answers to any questions from auditors, whatever the regulatory framework involved in the audit. UBCA solutions must provide rich and easy-to-use reporting for in-depth audit.

4. Reducing the number of fraudulent behaviors

Reducing the cost of fraud requires identifying the root cause of noncompliance.

Mitigating the risk of fraud requires controlling the access to sensitive information. UBCA solutions must also accelerate response to fraud through real-time dashboards and alerts.

The REQUIREMENTS volume provides the detailed requirements.

Comments

The detailed assessment of the shortlisted solutions demonstrates that the best ones have the strengths that would be useful for large companies and would represent a valuable investment. The assessment results demonstrate that the shortlisted solutions are valuable. However, there are significant differences among the solutions in the coverage of the different assessment dimensions.

We remind you that building a Proof of Concept in the targeted technical environment and for the expected value-added benefits remains a requirement.

- **Tivoli Compliance Insight Manager (IBM)** provides the best coverage of our list of requirements. This highlights its maturity and reliability for investing in this market segment.

  We appreciate IBM Tivoli clear vision and understanding of this business case and the well-centered strategy. Tivoli Compliance Insight Manager is clearly positioned on compliance issues and the audit of user behavior.

  We appreciate how Tivoli Compliance Insight Manager facilitates the investigation thanks to out-of-the-box features. TCIM is designed to support a high volume of activity. Log integrity is guaranteed, from source to long-term storage. TCIM strengths include ease to query thanks to a comprehensive and unique logs format (after normalization), the richness of the compliance reports and the ease to write rules for investigation based on a powerful correlation engine.

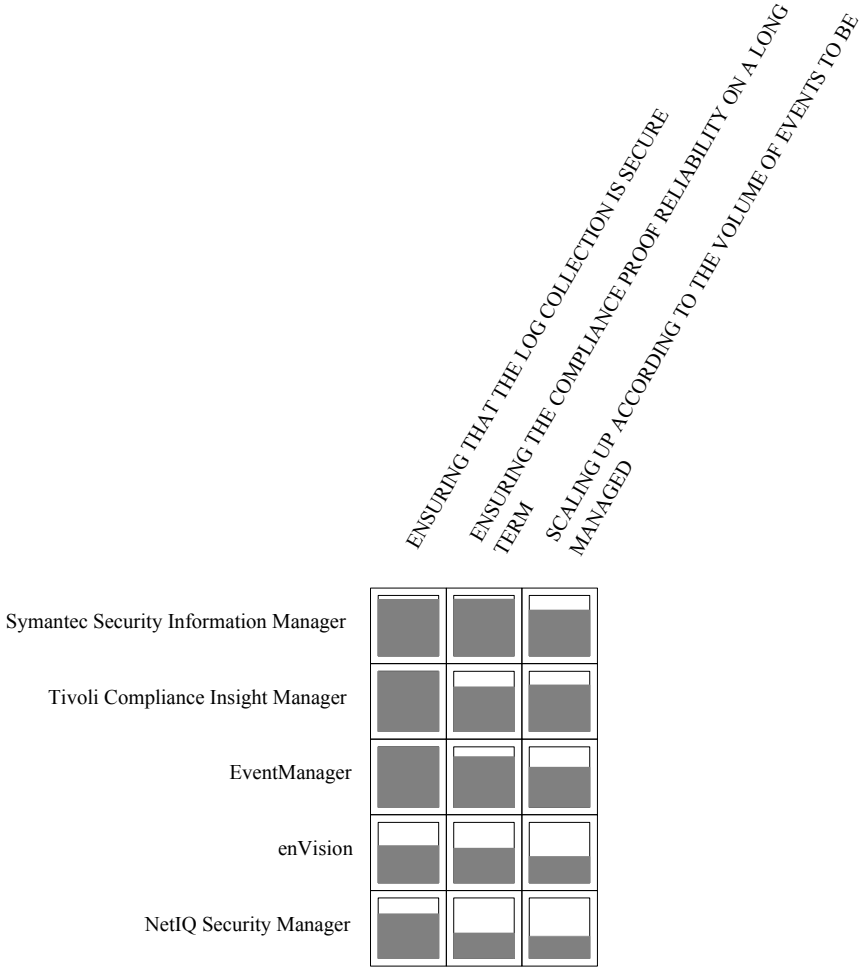
- **EventManager (Exaprotect)** demonstrates advanced capabilities in our four assessment dimensions. The strengths of Exaprotect are the interfaces, the ease of use and the numerous wizards to facilitate queries and reporting. Exaprotect provides a rich correlation engine, which makes it possible to define behaviors and exceptions. Exaprotect natively integrates useful functions for achieving and demonstrating quickly and efficiently user behavior compliance according to regulatory requirements or company policies.

- **Symantec Security Information Manager (Symantec)** has good coverage of our list of requirements. It stands out in "Ensuring a secure log collection'', thanks to high performance in collecting the data and to a context-based collection policy. We appreciate how the correlation rule engine manages the level of severity or priority according to many event attributes. We appreciate the use of Global Intelligence Networks to take into account risk information from external sources.

- **enVision (EMC)** is a valuable solution. The solution is security-oriented. It provides good capabilities for log management and has strength in collecting a high volume of events. The solution can treat and manage a high volume of data very quickly. We appreciate the numerous out-of-the-box reports, including regulatory framework reports.

- **NetIQ Security Manager (Attachmate)** is a valuable solution. We appreciate the trend analysis and the forensic representation based on OLAP cube. This function is easy to use and provides quickly a friendly graphical representation. Another strength of NetIQ Security Manager is a knowledge base that can be customized for each company. Access to the knowledge base is controlled according to the roles. This contributes to the continuous improvement of the solution.

1. ENSURING A SECURE LOG COLLECTION



1. ENSURING A SECURE LOG COLLECTION

1.1 There are differences among the shortlisted solutions in "Ensuring that the log collection is secure". The best solutions ensure the integrity of raw logs whatever the log origins and formats are. They provide out-of-the-box connectors and facilitate and ensure collection from heterogeneous sources.

1.2 There are significant differences among the shortlisted solutions in "Scaling up according to the volume of events to be managed''. The best solutions provide flexible architecture in order to support a huge volume of data during log collection.

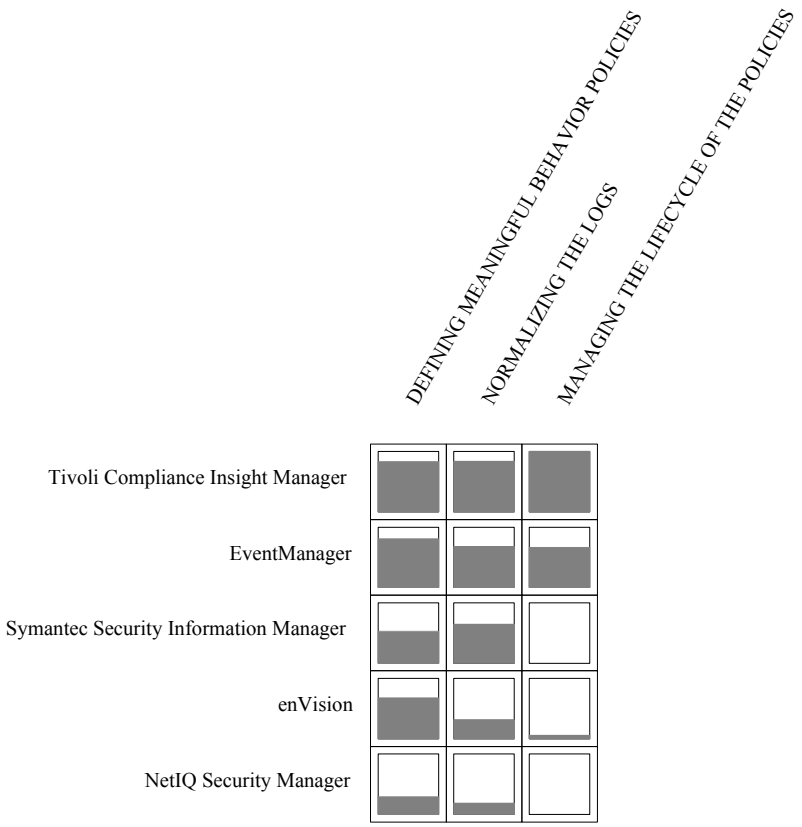
1.3 There are significant differences among the shortlisted solutions in "Ensuring the compliance proof reliability on a long term''. The best solutions store the data and ensure security by encryption, compression and access control.

- **Tivoli Compliance Insight Manager** ranks high in the three dimensions. It provides very good coverage of this part of our list of requirements. Collection can be scheduled independently for each collector. We appreciate how TCIM ensures data transfer from source to console by encrypting and compressing the data. TCIM also has good capabilities in ensuring the data storage and provides accurate access control to this data. TCIM ensures that the raw logs keep their integrity.

- **EventManager** ranks high in the three dimensions. We appreciate the collection policies that help define how to collect and ensure security and performance. The solution has good capabilities in securing the data storage by encryption and signing. The solution time-stamps raw data. We also appreciate the graphical representation of the log continuity report. This provides user-friendly representation of the data volume or the bottlenecks. It helps ensure compliance of log collection.

- **Symantec Security Information Manager** has the best coverage of this part of our list of requirements. Many customized options are accessible to define the collection policies. We appreciate the Statistic Viewer, which allows the tracking of collection and provides a graphical representation of the log collection (status, name, total of processed events and so on).

2. DEFINING THE COMPLIANT BEHAVIOR POLICIES



2. DEFINING THE COMPLIANT BEHAVIOR POLICIES

2.1 There are significant differences in "Normalizing the logs''. The best solutions centralize the logs in a unique format that nontechnical people can understand.

2.2 There are significant differences in "Defining meaningful behavior policies''. The strengths of best solutions are data correlation and aggregation, as well as definition of behavior policies.

2.3 There are significant differences in "Managing the lifecycle of the policies''. Only two solutions cover this part of our list of requirements. They provide easy-to-use tools to manage several behavior policies and manage them according to the context. They also manage those policies during their lifecycle by versioning them.

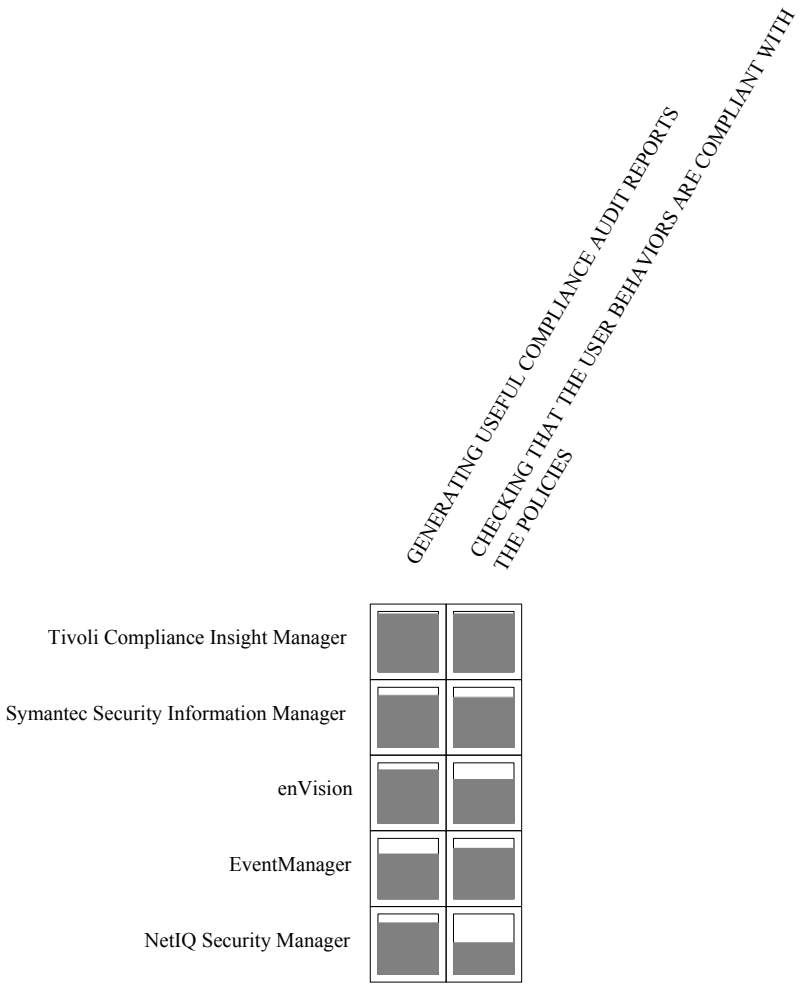
- **Tivoli Compliance Insight Manager** stands out in these three dimensions. It demonstrates good capabilities for defining a central and unique format of the logs. It makes the normalized logs available and understandable to auditors. It helps define the usual behaviors (through the policies), even if the sources are heterogeneous. Therefore, TCIM has strengths in detecting the abnormal behaviors independently of the platforms, the format or the volume of activity.

  We also appreciate that the solution distinguishes between a test/simulation and the operational environments.

- **EventManager** has good coverage of this part of our list of requirements. We appreciate the business asset database provided by the solution. A business asset is a company item on which threats and vulnerabilities are under control, identified and calculated to evaluate the risk. We also appreciate the log analysis performed by agents, which allows filtering the criticality level setting. The solution allows makes it possible to define scenarios corresponding to user behavior and therefore detect a risk based on complex correlation rules.

- **Symantec Security Information Manager** has good coverage of this part of our list of requirements, thanks to out-of-the-box "User Lookup Tables", e.g. weekdays, IP watchlist, sensitive data. These can be enriched manually or by the Global Intelligence Network. Symantec provides normalization of logs according to EMR (Effect - Mechanism - Resources) concepts (according to DMTF standards). The solution has good capabilities for rule optimizing.

3. AUDITING THE COMPLIANCE WITH POLICIES



3. AUDITING THE COMPLIANCE WITH POLICIES

3.1 There is no significant difference among the shortlisted solutions in "Checking that the user behaviors are compliant with the policies". All the shortlisted solutions provide out-of-the-box reports to demonstrate compliance with regulatory frameworks. The difference lies in the accuracy and ease of demonstrating the compliance.

3.2 There are differences among the shortlisted solutions in "Generating useful compliance audit reports". Some solutions provide powerful reporting tools.

- **Tivoli Compliance Insight Manager** has the best coverage of this part of our list of requirements. TCIM provides a graphical and easy-to-use representation of the situation, highlighting the noncompliant actions. We appreciate the capability to drill down from incidents to raw logs. The solution facilitates customization of reports based on the 7 Ws (who, what, on what, when, where, from where, where to), thanks to the report editor. TCIM has also interesting functions for scheduling**.**

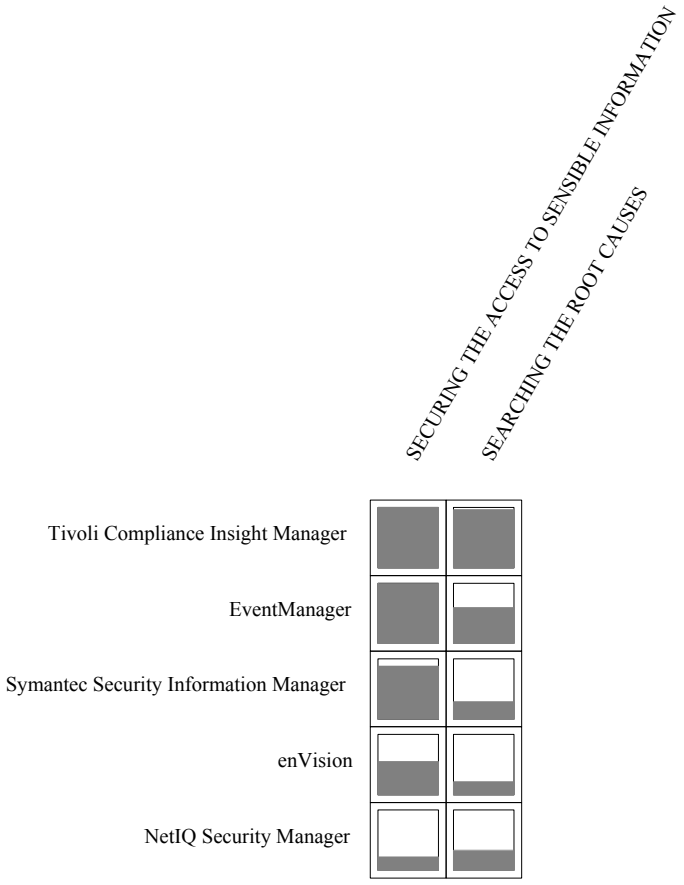
- **EventManager** ranks low in this part of our list of requirements. However, we appreciate the numerous out-of-the-box reports demonstrating the compliance with regulatory frameworks and the reports that focus on privileged user behaviors. Exaprotect has seamless integration with Prelytis for reporting. Therefore, it provides powerful capabilities in order to custom the reports.

- **Symantec Security Information Manager** has good coverage of this part of our list of requirements. We appreciate the automatic setting of the severity or priority level based on the correlation of various event attributes. We also appreciate how the reporting tools demonstrate compliance to auditors.

- **enVision** has good coverage of this part of our list of requirements. We appreciate the numerous out-of-the-box reusable reports, including around 60 reports on regulatory frameworks (Basel II, SOX and so on).

- **NetIQ Security Manager** ranks low in this part of our list of requirements. However, Attachmate is involved in the continuous improvement strategy through the knowledge base. We appreciate the capability to create a specific knowledge base for each company. This base is accessible according to role-based access control. We also appreciate the easy-to-use reporting tools (trend analysis and forensic reports) based on OLAP cubes.

4. REDUCING THE NUMBER OF FRAUDULENT BEHAVIORS



Sorted Aggregated Table

4. REDUCING THE NUMBER OF FRAUDULENT BEHAVIORS

4.1 There are very significant differences among the shortlisted solutions in "Searching the root causes''. Most solutions provide powerful tools for searches via queries. However, only one solution supports comparisons between the actual and the usual situation followed by a clear tool of investigation.

4.2 There are differences among the shortlisted solutions in "Securing the access to sensitive information''. They all provide role-based access control. However, all the solutions vary in comprehensiveness of provided functions. Indeed, some solutions provide finer granularity.

- **Tivoli Compliance Insight Manager** stands out clearly in both dimensions. The solution has an easy-to-use investigation function that can find the root cause of abnormal behaviors. It can focus on the root cause according to user or according to complex queries. The focus on policy violations is clear and makes it possible to drill down to the raw data. Tivoli Compliance Insight Manager also provides granular role-based access in order to secure the sensitive data.

- **EventManager** ranks average in "Searching the root causes'' and has good coverage of "Securing the access to the sensitive information''. The solution can control access rights until the final reports. It provides a finer granularity in its access control management.

- **Symantec Security Information Manager** ranks low in "Searching the root causes'' and has good coverage of "Securing the access to the sensitive information''. We appreciate the access control on the archive, which makes it possible to define the priority level on specific data.

The ASSESSMENT volume provides the detailed assessment of each shortlisted solution.